REMARKS

Claims 1-5, 8-14, 17-19, 26-30, 33-39 and 42-44 are pending in the present application. Claims 1, 8, 11, 17, 18, 26, 33, 36, 42 and 43 have been amended, and Claims 6-7, 15-16, 20-25, 31-32, 40-41 and 45-46 have been cancelled, herewith. Reconsideration of the claims is respectfully requested. In addition, Applicants request that this amendment after final be entered as placing this case in condition for allowance or better form for appeal.

I. Specification

The Examiner notes the use of Java on page 8 of the present Specification, and states that it should be capitalized wherever it appears and be accompanied by the generic terminology. Applicants have reviewed the use of Java on page 8, and note that it is capitalized at each instance of use, and in addition is accompanied by generic terminology ('object oriented programming system such as Java', 'Java programs or applications', '"Java" is a trademark'. Thus, the use of Java in the present Specification complies with the Examiner's requirements regarding capitalization and generic terminology.

II. 35 U.S.C. § 102, Anticipation

The Examiner rejected Claims 1-46 under 35 U.S.C. § 102(b) as being anticipated by US Patent 6,028,939 to Yin. This rejection is respectfully traversed.

With respect to Claim 1, Applicants have amended such claim to include the features previously recited in Claims 6 and 7 (which are thus being cancelled herewith). As amended, Claim 1 includes features of performing the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, and wherein the step of performing the cryptographic operation includes *converting the key to a form useable by the selected process if the key is in an unusable form by the selected process*. As can be seen, the key used in the cryptographic operation is conditionally converted to a form useable by a selected process if the key is in an unusable form by the selected process. This claimed feature advantageously and

synergistically co-acts with the selecting step that selects between a hardware and software process for performing a cryptographic operation based on a policy, in that the key is converted to a form usable by the selected process.

In rejecting Claim 7 (the feature of Claim 7 now being a part of amended Claim 1), the Examiner states Yin teaches the claimed key converting step at column 12, lines 5-25 and 45-67. Applicants show that there, Yen states:

> Microprocessor 221 does not have to be a particularly high powered processor in order to provide a high performance data security system. Microprocessor 221 may perform overhead functions to control the two processing systems. It may be a server, for example, that interfaces a private network (not shown) to a high speed ATM network. The microprocessor may execute public key functions, either alone or in combination with one or both of the processing systems 200 to perform **a key exchange operation to agree upon a particular session key and supply that session key to the appropriate one of the processing systems.** In this manner, microprocessor 221 can manage two different simultaneous data security processing operations being performed using two separate keys. As before, each processing system 200 may perform a DES data security operation by allocating the various functions and operations between the microprocessor 204 and the PHE 210 (FIG. 9). Alternatively, the PHE could perform not only the entire DES ECB operation, but also the cipher block chaining operation using an initial vector and subkeys provided by the microprocessor. (column 12, lines 5-25) (emphasis added by Applicants)

> This approach is also adaptable to processing operations other than data security, e.g., data compression. Operations, such as signal processing, employing fast Fourier transforms which require exponentiation are very inefficient when done in hardware. It is much more efficient to do such operations in software, e.g., with a Digital Signal Processor device. Accordingly, it would be appropriate to allocate such arithmetic operations to the microprocessor to perform, rather than having them done in the hardware PHE. Similarly, bit manipulation operations and table look-ups are very efficient in hardware, unless the table look-up varies constantly. In this case, it is not the same table, since the data is changing, and it may be more efficient to perform such operations in software. In table look-ups, if it would be necessary to use a RAM to implement the table, and it cannot be done one-time during system installation, it is better done in software than in hardware. On the other hand, if the table is static or key

> dependant, such as in the S-box operation of DES or other algorithms, then it is more efficient to implement such table look-ups in hardware. (column 12, lines 45-65)

The above listed passage from Yin column 12, lines 5-25 describes a 'key exchange' capability in which a particular session key is agreed to and provided to the appropriate processing system, thus providing an ability to simultaneously perform two data security processing operations. The above listed passage from Yin column 12, lines 45-65 describes various processes that are better suited for either hardware or software processing. Notably absent in both of these cited passages is any discussion of any type of key conversion, and in particular there is no teaching or suggestion of any step or means for encryption of data using a key which includes *converting the key to a form useable by the selected process if the key is in an unusable form by the selected process.* Rather, the cited passages merely teach that an appropriate key is agreed upon and supplied. For a prior art reference to anticipate in terms of 35 U.S.C. 102, every element of the claimed invention must be identically shown in a single reference. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990). As every element of the claimed invention is not identically shown in a single reference, it is shown that the cited reference does not anticipate amended Claim 1.

Applicants traverse the rejection of Claims 2-5, 9 and 10 for reasons given above with respect to Claim 1 (of which Claims 2-5, 9 and 10 depend upon).

With respect to Claim 8, Applicants have amended such claim to be in independent form, but have not substantively amended such claim as it is merely being amended as to form. For similar reasons to those given above regarding amended Claim 1, it is urged that the cited reference does not teach the claimed feature of "performing the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, wherein the key is a hardware key and the selected process is the software process and further comprising *converting the hardware key into a software form useable by the software process for performing the cryptographic operation*". Thus, Claim 8 is shown to not be anticipated by the cited reference, as every element of the claimed invention is not identically shown in a single reference.

With respect to Claim 11 (and dependent Claims 12-14 and 17-19), Applicants have amended such claim to include features previously recited in Claims 15 and 16 (which are thus being cancelled herewith). As amended, Claim 11 recites "performing the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, and wherein the step of performing the cryptographic operation includes converting the key to a form useable by the selected process if the key is in an unusable form by the selected process". Applicants traverse the rejection of Claim 11 (and dependent Claims 12-14 and 17-19) for similar reasons to those described above with respect to Claim 1.

With respect to Claims 20-25, Applicants are canceling such claims herewith without prejudice or disclaimer in order to allow this case to expeditiously pass to issuance.

With respect to Claim 26 (and dependent Claims 27-30 and 33-35), Applicants have amended such claim to include features previously recited in Claims 31 and 32 (which are thus being cancelled herewith). As amended, Claim 26 recites "performing means for performing the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, and wherein the performing means includes *converting means for converting the key to a form useable by the selected process if the key is in an unusable form by the selected process*". Applicants traverse the rejection of Claim 26 (and dependent Claims 27-30 and 33-35) for similar reasons to those described above with respect to Claim 1.

With respect to Claim 36 (and dependent Claims 37-39 and 42-44), Applicants have amended such claim to include features previously recited in Claims 40 and 41 (which are thus being cancelled herewith). As amended, Claim 36 recites "performing means for performing the cryptographic operation using the selected process, wherein the cryptographic operation is an encryption of data using a key, and wherein the performing means includes *converting means for converting the key to a form useable by the selected process if the key is in an unusable form by the selected process*". Applicants traverse the rejection of Claim 36 (and dependent Claims 37-39 and 42-44) for similar reasons to those described above with respect to Claim 1.

Therefore, the rejection of Claims 1-46 under 35 U.S.C. § 102 (b) has been overcome.

III. Conclusion

It is respectfully urged that the subject application is patentable over the cited refcrence and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: 2/15/05

Respectfully submitted,

Duke W. Yee
Reg. No. 34,285
Wayne P. Bailey
Reg. No. 34, 289
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorneys for Applicants